International Journal of Technological Exploration and Learning (IJTEL)
Volume 2 Issue 4 (August 2013)

Multicasting Hierarchical Routing Protocol of Mobile Ad Hoc Networks

B. Swetha
Assistant Professor, Department of Computer Science
Gnyana Saraswati College of Engineering & Technology
Nizamabad. Andhra Pradesh, India

***Abstract*— A Mobile adhoc network (MANETs) is a collection of wireless mobile nodes dynamically forming a network without using any centralized access point, infrastructure or centralized administration multicasting is an useful operation that facilitates group communication efficient and scalable .Multicast routing in MANETs is a difficult issue. In addition to the conventional multicast routing algorithms, recent protocols have adopted are overlays, backbone-based, and stateless.To enhance performance and enable scalability, we have proposed a framework for hierarchical multicasting in MANETs environment. Two classes of hierarchical multicasting approaches termed as domain based and overlay-based are proposed. We have considered a verity of approaches that are suitable for different mobility patterns and multicast group size.**

Keywords-component; formatting; style; styling; insert (key words)

I. INTRODUCTION

There are currently two variations of mobile wireless networks infrastructured and Infrastructureless networks. The infrastructured networks, also known as Cellular network, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local, area networks (WLANs). The other type of network, Infrastructureless network, is known as Mobile Ad NETwork (MANET). These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

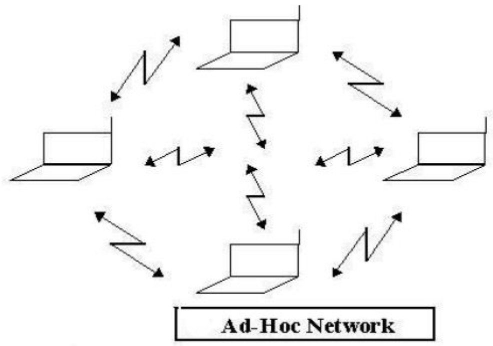

Figure 1. Ad Hoc Network

The chief difference between ad hoc networks is the apparent lack of a centralized entity within an ad hoc network. There are no base stations or mobile switching centers in an ad hoc network.

The interest in wireless ad hoc networks stems from of their well-known advantages for certain types of applications. Since, there is no fixed infrastructure, a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons. Ad-hoc networks were mainly used for military applications. Since then, they have become increasingly more popular within the computing industry. Applications include emergency search and rescue operations, deployment of sensors, conferences, exhibitions, virtual classrooms and operations in environments where construction of infrastructure is difficult or expensive. Ad-hoc networks can be rapidly deployed because of the lack of infrastructure.

II. RACTERISTICS OF MANET

A. Dynamic Topologies

Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional bidirectional.

B. Bandwidth constrained, variable capacity links

Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

C. Energy constrained operation

Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

D. Limited physical security

Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.

III. MULTI-HOP WIRELESS AD HOC NETWORK ROUTING PROTOCOLS

Multihop or adhoc,wireless networks use two or more wireless hops to convey information from a source to a destination .There are two distinct application of Multi-hop communication with common features, but different application. Mobile ad-hoc networks: A mobile adhoc networks consists of a group of mobile nodes that communicates without requiring a fixed wireless infrastructure.In contrast to conventional cellular systems there is no master-slave relationship between nodes such as o'base static to mobile users in adhoc networks. Communication between nodes is performed by direct connection or through multiple-hop relays. MANETs network have several practical application including battle field communication, emergency first response and public safety system. Despite extensive research in networking, many challenges remain in the study of mobile adhoc network including development of multiple access protocols that exploit advanced physical layer technologies like MIMO,OFDM and interference cancellation, analysis of the fundamental limits of mobile ad-hoc network capacity practical characterization of achievable throughputs taking into account network

MIMO: Multiple-Input and Multiple-Output.

OFDM: Orthogonal Frequency Division Multiplexing.

In this paper, we focus on the area of secure routing protocols for ad hoc networks. First, given model describes the possible types of attacks in such a system and depict several new attacks on ad hoc network routing protocols. And next we are with multi-hop wireless networking and we are describes the protocols and issues of multicast routing protocols with manets

A. Various Existed On-Demand Secure Routing Protocols

Mobile ad hoc networks are vulnerable to various security threats because of its dynamic topology and self-configurable nature. Several researchers have proposed secure routing protocols. In that we have used many routing algorithm and all these secure routing protocols that have been proposed to reduce the risk of attacking the routing protocols. Many secure routing protocols aim to prevent the establishment of falsified routes.

1) ARAN Protocol

The Authenticated Routing for Ad-Hoc Networks (ARAN)[4],[8],[11] secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the ad hoc environment and consists of a preliminary certification process, a mandatory end to-end authentication stage and an optional second stage that provides secure shortest paths.

2) SAODV Protocol

SAODV (Secure Ad hoc On Demand Vector routing) Protocol is an implementation of SAR on AODV. It is one of the popular secure mechanisms which take the help of digital signature and hash chain techniques to secure AODV packets. Since, digital signature technique consumes heavy computational time, the degradation of SAODV performance can be a major issue.

3) SRP Protocol

Source routing protocols (SRP) prevents spoofing attacks. T his protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

4) ARIADNE Protocol

It is an on-demand secure adhoc routing protocol based on DSR that withstands node compromise and relies only on highly efficient symmetric cryptography. ARIADNE provides point-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties. For authentication of a broadcast packet such as RREQ, ARIADNE uses the TESLA broadcast authentication protocol. Selfish nodes are not taken into account.

5) SAR Protocol

Security-Aware Ad-Hoc Routing protocol is the generalized framework for any on demand ad-hoc routing protocol. SAR requires that nodes having same trust level must share a secret key. SAR augments the routing process using hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity while the encryption of packets ensures their confidentiality**.**

6) SLSP Protocol

Secure Link State Routing Protocol provides secure proactive topology discovery and can be used as either as a stand-alone protocol or as a part of Hybrid routing framework when combined with a reactive protocol.

7) ABV Model

The ABV model [1],[2],[4],[6],[7] is a security framework proposed by Acs, Buttyan and Vajda[1] used to analyze on-demand routing algorithms, SRP and Ariadne and finds them insecure against hidden channel attacks. ABV proposed to merge faulty neighbor nodes into a single node. So the neighbor nodes of a faulty node on a route are not faulty. Consequently, adversarial nodes are, by definition, never adjacent in the ABV model. This is an arbitrary restriction therefore incomplete. It could be possible that the security claims remained valid even as their proof is incorrectly argued. Fundamentally, end air A and the ABV model was developed to deal with a class of hidden channels, the intrinsic hidden channels of a wireless broadcast medium in a neighborhood. However, security is not achieved

because other hidden channels remain present that greatly limits the scope of the security statements in the ABV model in their ability to capture realistic security requirements.

It is concluded that the proof makes the unwarranted assumption that no direct channels imply no direct bandwidth between adversarial nodes.

IV. MULTICASTING IN MANETSTATE MANAGEMENT AND SCALABILITY

State management of multicast protocols involves timely updating of the multicast routing tables at the involved nodes to maintain the correctness of the multicast routing structure, tree or mesh, according to the current network topology. Even under moderate node mobility and multicast member size, state management incurs considerable amount of control traffic. When the group size grows, and/or number of groups increase, traditional tree or mesh based methods [24], [25], [26] become inefficient. To address the scalability issues, we need to reduce the protocol states and constrain their distribution, or even use methods that do not need to have protocol state. A number of research efforts have adopted this method, which can be classified into the following categories: overlay multicasting, backbone-based multicasting and stateless multicasting. We study these different approaches for constraining protocol states, and their scalability issues different approaches for constraining protocol states, and their scalability issues

A. Overlay multicast routing protocols

In overlay multicast, a virtual infrastructure is built to form an overlay network on top of the physical network. Each link in the virtual infrastructure is a unicast tunnel in the physical network. IP layer implements minimal functionality– a best-effort unicast datagram service, while the overlay network implements multicast functionalities such as dynamic membership maintenance, packet duplication and multicast routing. AMRoute[27] is an ad hoc multicast protocol that uses the overlay multicast approach. The virtual topology can remain static even though the underlying physical topology is changing. Moreover, it needs no support from the non-member nodes, i.e., all multicast functionality and protocol states are kept within the group member nodes. The protocol does not need to track the network mobility since it is totally handled by the underlying unicast protocol.

The advantages of overlay multicast come at the cost of low efficiency of packet delivery and long delay. When constructing the virtual infrastructure, it is very hard to prevent different unicast tunnels from sharing physical links, which results in redundant traffic on the physical links. Besides, the problem of low delivery efficiency is discussed

B. Backbone-based Multicast Protocols

For a backbone-based approach, a distributed election process is conducted among all nodes in the network, so that a subset of nodes are selected as CORE nodes. The topology induced by the CORE nodes and paths connecting them form the virtual backbone, which can be shared by both unicast and multicast routing. In MCEDAR[28], a distributed minimum dominating set (MDS) algorithm1 is applied for this purpose, and the resulting backbone has the property that all nodes are within one hop away from a CORE node. A CORE node and its dominated nodes form a cluster. The proposed protocol in [29] and [30] use different techniques for selecting backbone nodes. Once a virtual backbone is formed, the multicast operation is divided into two levels. The lower level multicast, which is within a cluster, is trivial. For the upper level multicast, the protocol in [29] uses a pure flooding approach within the backbone.MCEDAR builds a routing mesh, named as mgraph, within the virtual backbone, to connect all CORE nodes. The backbone topology is much more simple and stable than the whole network topology. If backbone are built upon slowmoving nodes, more topology stability is expected even with high host mobility. However, backbone-based method makes each CORE node a “hot-spot” of network traffic, which poses limits on horizontal scalability. Backbone-based protocols are limited for supporting horizontal scalability. Since data traffic of all the multicast groups should pass the same set of CORE nodes, the number of multicast groups that can be supported by the network is limited by the channel bandwidth at each CORE node.

C. Stateless Multicast Protocols

A recent shift towards stateless multicasting is represented by DDM[31], LGT[32] and RDG[33]. All these protocols do not require maintenance of any routing structure at the forwarding nodes. These protocols use different techniques to achieve stateless multicasting. LGT builds an overlay packet delivery tree on top of the underlying unicast routing protocol, and multicast packets are encapsulated in a unicast envelop and unicasted between the group members. When an on-tree node receives a data packet from its parent node, it gets the identities of its children from the infomation included in the header of the packet For RDG, a probabilistically controlled flooding technique, termed as gossiping, is used to deliver packets to all the group members. In DDM, a source encapsulates a list of destination addresses in the header of each data packet it sends out. When an intermediate node receives the packet, its DDM agent queries the unicast routing protocol about which next-hop node to forward the packet towards each destination in the packet header. DDM is intended for small groups, therefore, it intrinsically excels only in horizontal scalability. When group size is large, placing the addresses of all members into the packet headers will not be efficient. The protocol has a caching mode, so that only the difference from the previous states is actually placed in the headers. However, as the forwarding set at the on-route nodes inevitably grow large, each intermediate node needs to keep routes for a large set of destinations.

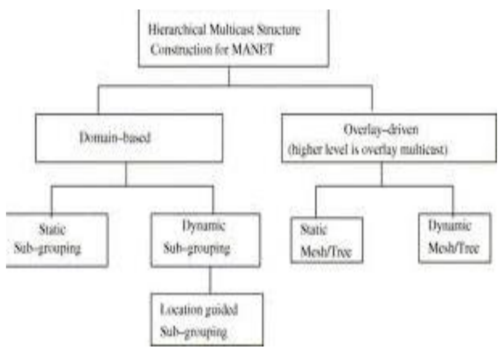

Figure 2. Different manners of constructing hierarchical multicast trees

This poses a heavy burden on the supporting unicast protocol even under moderate mobility. Further, in order to answer the “next-hop” queries for a large number of destinations, on-demand routing protocols, which are

commonly proposed for MANETs, need to flood the entire network very frequently with route discovery packets.

V. HIERARCHICAL MULTICASTING

Hierarchical routing[34] approach can be used to significantly reduce the protocol states in a large scale network. In this section, we present two hierarchical multicast solutions, both of which have the goal of achieving lower multicast overhead and robustness for large-scale multicasting. We refrainframework, a variety of techniques can be adopted for effective multicasting in MANETs. A critical component of hierarchical multicasting in MANETs involves the way the multicast tree or mesh are constructed. For the proposed framework, we have formed a generic classification of various possible configurations of hierarchical multicasting in MANETs. This classification is depicted in Figure 1. The approaches differ in the relationship between two adjacent levels of multicast trees, i.e., how the lower level multicast trees are organized to serve the upper level. In this section, we describe the methodologies of these multicasting techniques

VI. SINGLE AND MULTIPLE SOURCE MULTICAST ROUTING PROTOCOLS

A multicast group may contain multiple sources due to different kinds of services or applications simultaneously provided by the networks. Each single source multicast routing protocol induces a lot of overhead and thus wastes tremendous network resources in multi-source multicast environments. In multiple source multicast routing protocols using the clustering technique, a large network can be divided into several sub-networks with only a few cluster heads needing to maintain local information, thus preventing flooding of useless packets and avoiding wasting bandwidth. To achieve efficient multicasting in a multi-source multicast environment, the clustering technique is employed to design an efficient multicast routing protocol for multisource multicasting. Cluster and multicast path maintenance is expected to adapt dynamic network topology . Multiple source routing is essential for load balancing and offering quality of service. Other benefits of multiple source routing include: the reduction of computing time that routers' CPUs require, high resilience to path breaks, high call acceptance ratio (in voice applications) and better security. Special attention should be given to transport layer protocols as duplicate acknowledgments could occur, which might lead to excessive power consumption and congestion

VII. ISSUES IN DESIGNING A MULTICAST ROUTING PROTOCOL

- Limited bandwidth availability, an error-prone shared broadcast channel, the mobility of nodes with limited energy resources, the hidden terminal problem [5], and limited security make the design of a multicast routing protocol for ad hoc networks ina challenging one. There are several issues volved here which are discussed below.

- Robustness: Due to the mobility of the nodes, link failures are quite common in ad hoc wireless networks. Thus, data packets sent by the source may be dropped, which results in a low packet delivery ratio. Hence, a multicast routing protocol should be robust enough to sustain the mobility of the nodes and achieve a high packet delivery ratio.

- Efficiency: In an ad hoc network environment, where the bandwidth is scarce, the efficiency of the multicast protocol is very important. Multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of (data and control) packets transmitted in the network.

- Control overhead: In order to keep track of the members in a multicast group, the exchange of control packets is required. This consumes a considerable amount of bandwidth. Since bandwidth is limited in ad hoc networks, the design of a multicast protocol should ensure that the total number of control packets transmitted for maintaining the multicast group is kept to a minimum.

- Quality of service: One of the important applications of ad hoc networks is in military/strategic applications. Hence, provisioning quality of service (QoS) is an issue in ad hoc multicast routing protocols. The main parameters which are taken into consideration for providing the required QoS are throughput, delay, delay jitter, and reliability.

- Dependency on the unicast routing protocol: If a multicast routing protocol needs the support of a particular routing protocol, then it is difficult for the multicast protocol to work in heterogeneous networks. Hence, it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol.

- Resource management: Ad hoc networks consist of a group of mobile nodes, with each node having limited battery power and memory. An ad hoc multicast routing protocol should use minimum power by reducing the number of packet transmissions. To reduce memory usage, it should use minimum state information.

VIII. CONCLUSION

In this paper, we apply the Multicast hierarchical routing of MANETS. We categorize the current paper with mobile Adhoc routing protocols and multicast routing protocols with MANETS. We also study the scalability of State Management of Multicasting and Issues in Designing a Multicast Routing Protocols.

The future works, we identify the need to develop a better reliability in packet delivery by using multicast hierarchy routing protocols of MANETS

REFERENCES

[1] G.Acs, L. Buttya´n, and I. Vajda, "ProvableSecurity of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks".

[2] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks".

[3] G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad HocNetworks".

[4] Acs, L. Buttya´n, and I. Vajda, "Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks".

[5] M. Burmester, T. van Le, and A. Yasinsac,"Adaptive Gossip Protocols: Managing Security and Redundancy in Dense Ad Hoc Networks".

[6] L. Buttya´n and I. Vajda, "Towards Provable Security for Ad Hoc Routing Protocols".

[7] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc

[8] Y.-C. Hu, A. Perrig, and D. Johnson, "A Survey of Secure Wireless Ad Hoc Routing Protocols".

[9] D. Johnson and D. Maltz, "Dynamic SourceRouting in Ad Hoc Wireless Networks".

[10] P. G. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," *IEEECommunications Surveys & Tutorials*, vol. 7, no. 3,2005, pp. 2-21.

[11] B. Dahill, B. N. Levine, E. Royer, and C. Shields. Aran:A secure routing protocol for ad hoc networks.TechnicalReport UMass Tech Report 02-32, University of Massachusetts, Amherst, 2002

[12] .J. Marshall, V. Thakur, and A. Yasinsac,"Identifying flaws in the secure routing protocol,"in *Proc. 2003 IEEE International Performance,Computing,andCommunicationsConference*,2003, pp. 167-174.

[13] G. Ács, L. Buttyán, and I. Vajda, "Provably secure on-demand source routing in mobile adhoc networks," *IEEE Transactions on MobileComputing*, vol. 5, no. 11, 2006, pp. 1533-1546.

[14] L. Buttyán and I. Vajda, "Towards provable security for ad hoc routing protocols," in *Proc.2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004, pp. 94-105.

[15] J. Marshall, V. Thakur, and A. Yasinsac, "Identifying flaws in the secureroutingprotocol,"in*Proc.2003IEEEInternationalPerformance,Computing,and Communications Conference*, 2003, pp. 167-174.

[16] G. Ács, L. Buttyán, and I. Vajda,"Provably secure on-demand source routing inmobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, 2006, pp. 1533-1546.

[17] G. Ács, L. Buttyán, and I. Vajda, "Provable security of on-demand distance vector routing in ad hoc networks," in *Proc. European Workshop on Security and Privacy*, 2005, pp. 113-127.

[18] P. Rreyan and S. Schneider, *Modelling and Analysis of Security Protocols*. Harlow, England: Addison-Wesley, 2001.

[19] S. Nanz and C. Hankin, "A framework for security analysis of mobile wireless networks,"*Theoretical Computer Science*, vol. 367, no. 1-2, 2006, pp. 203-227.

[20] S. Nanzre, "Specification and Security Analysis of Mobile Ad-Hoc Networks," Ph.D. Thesis,Department of Computing Imperial College London, 2006.

[21] P. Ramachandran and A. Yasinsac, "Limitations of on demand secure routing protocols," in *Proc. Fifth Annual IEEE SMC Information Assurance Workshop*, 2004, pp. 52-59.

[22] T. R. Andel and A. Yasinsac, "The Invisible Node Attack Revisited," in *Proc. 2007 IEEE SoutheastCon*, 2007, pp. 686-691

[23] P. Maggi and R. Sisto, "Using SPIN to Verify Security Properties of Cryptographic Protocols," in *9th international SPIN Workshop on Model Checking of Software*, vol. 2318,*LNCS*: Springer-Verlag, 2002, pp. 187.

[24] E. M. Royer, and C. E. Perkings, "Multicast Operations of the Adhoc On-Demand Distance Vector Routing Protocol," *Proc. ACM MOBICOM' 99,* Seattle, WA, Aug., 1999.

[25] J. J. Garcia-Luna-Aceves, and E. L. Madruga, "The Core-Assisted Mesh Protocol," *IEEE J. Select. Areas Commun.*, Vol. 17, No. 8, pp. 1380-94, August 1999.

[26] S.K. Das, B.S. Manoj, and C.S.R. Murthy, "A Dynamic Core Based Multicast Routing Protocol for Ad hoc Wireless Networks," *Proc. ACM MOBIHOC'02,* Lausanne, Switzerland, June 2002.

[27] J. Xie, R. R. Talpade, A. Mccauley, and M. Liu, "AMRoute: ad hoc multicast routing protocol," *ACM Mobile Networks and Applications,* Vol. 7, Issue 6, Dec. 2002.

[28] P. Sinha, R. Sivakumar and V. Bharghavan, "MCEDAR: Multicast Core- Extraction Distributed Ad Hoc Routing," *Proc. IEEE WCNC'99,* Sept., 1999.

[29] C. Jaikaeo and C-C. Shen, "Adaptive Backbone-Based Multicast for Ad hoc Networks," *Proc. IEEE ICC'02,* New York, NY, Apr.-May, 2002.

[30] M. Gerla, C-C. Chiang and L. Zhang, "Tree multicast strategies in mobile, multihop wireless networks," *ACM Mobile Networks and Applications,* Vol. 4, 1999, pp 193-207

[31] L. Ji and M. S. Corson, "Differential Destination Multicast -A MANET Multicast Routing Protocol for Small Groups," *Proc. IEEE Infocom'01,* Anchorage, Alaska, Apr., 2001.

[32] K. Chen and K. Nahrstedt, "Effective Location-Guided Tree ConstructionAlgorithms for Small Group Multicast in MANET," *Proc. IEEE Infocom'02,* New York, NY, June, 2002.

[33] J. Luo, P. T. Eugster, and J.-P. Hubaux, "Route Driven Gossip: Probabilistic Reliable Multicast in Ad Hoc Networks," *IEEE Infocom'03,* San Francisco, CA, Mar.-Apr., 2003.

[34] L. Kleinrock and F. Kamoun, "Hierarchical Routing for large networks;performance evaluation and optimization," Computer Networks, Vol. 1, pages 155-174, 1977